

CP:DAL
F#

M-11-229

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - -X

UNITED STATES OF AMERICA

- against -

AFFIDAVIT IN SUPPORT
OF APPLICATION FOR
SEARCH WARRANT

ONE MACBOOK PRO LAPTOP COMPUTER,
SERIAL NUMBER W87470VSXA9

(T. 18, U.S.C.,
§ 1029(a))

- - - - -X

EASTERN DISTRICT OF NEW YORK, SS:

MICHAEL ZAPPEL, being duly sworn, deposes and says that he is a Special Agent with United States Secret Service, Department of Homeland Security ("Secret Service"), duly appointed according to law and acting as such. I make this affidavit in support of an application for a search warrant for a laptop computer seized by the United States Office of Probation ("Probation") on or about January 29, 2008 from ASHLEY SIMMONS. At that time SIMMONS was on supervised release in connection with his December 1, 2005 conviction for conspiracy to commit access-device fraud pursuant to 18 U.S.C. § 371. On May 29, 2009, SIMMONS was indicted for participating in another access-fraud device scheme involving stolen credit-card information. On July 13, 2009, Simmons pleaded guilty to one count of access-device fraud pursuant to 18 U.S.C. § 1029, in a connection with that

scheme. SIMMONS' girlfriend and alleged co-conspirator, WINSOME WHITE, is scheduled to stand trial on March 14, 2011 on access-fraud, aggravated identity theft and false-statement charges.

Upon information and belief, there is probable cause to believe that the ONE MACBOOK PRO LAPTOP COMPUTER, SERIAL NUMBER W87470VSXA9 (the "SUBJECT COMPUTER") seized by Probation on January 29, 2008 from ASHLEY SIMMONS contains evidence and instrumentalities of an access-device fraud scheme involving WHITE and others.

I. Introduction and Background

1. I have been a Special Agent with the Secret Service for approximately four years. During my career, I have participated in numerous investigations concerning credit-card fraud and other access-device fraud crimes. In the course of my investigations, I have: a) conducted physical surveillance, b) participated in undercover transactions, c) executed search warrants, d) interviewed informants and cooperating witnesses regarding methods of committing access device fraud and e) reviewed taped conversations and records related to criminal activities including access-device fraud. Based on my experience, it is my belief that, in light of the information learned in this investigation, there is probable cause to believe that the SUBJECT COMPUTER was used to effect credit-card fraud,

3

and to store electronic information relating to the activities of the credit-card fraud conspiracy. It has been my experience that those who commit credit-card fraud often use computers to do so and often store electronic information relating to their criminal schemes on computers.

2. I have personally participated in the Secret Service investigation of the offense referred to above. From that participation and from reports made to me by other law enforcement officers, I am familiar with the facts and circumstances of this investigation. Because this affidavit is being submitted for the limited purpose of seeking a search warrant, I have not set forth each and every fact learned during the course of this investigation, but simply those facts which I believe are necessary to establish probable cause to support the issuance of a search warrant of the SUBJECT COMPUTER. Except where otherwise noted, all conversations described in this affidavit are set forth in part and in substance only.

3. As set forth below, there is probable cause to believe that the SUBJECT COMPUTER was used in furtherance of the access-device fraud scheme involving stolen credit-card information. Moreover, there is probable cause to believe that the SUBJECT COMPUTER contains information, i.e., stored e-mail

messages, address books, and other data, which demonstrates that the computer was used in furtherance of access-device fraud.

II. Facts Supporting Probable Cause

4. On December 1, 2005, ASHLEY SIMMONS was convicted of conspiracy to commit access-device fraud in the United States District Court for the Southern District of New York, and sentenced to 30 months' imprisonment, to be followed by three years of supervised release. SIMMONS was released from prison in or about May 2007.

5. On or about January 29, 2008, in the regular course of his duties monitoring SIMMONS' supervised release, United States Probation Officer Richard Koury visited SIMMONS at his apartment in Brooklyn, New York. As Koury entered the apartment, SIMMONS quickly ran towards the back of the apartment into his bedroom. Koury followed SIMMONS into the bedroom. In the bedroom, Koury observed a computer laptop case on the bed. During previous visits, SIMMONS had denied to Koury that he owned a computer. Koury asked SIMMONS whether he had a computer in the room. SIMMONS denied it. SIMMONS appeared nervous and seemed to be attempting to block Koury's access to the side of the bed. After moving past SIMMONS, Koury found the SUBJECT COMPUTER underneath the bed, with its power cord still connected to the wall outlet. At that point, SIMMONS grabbed the computer and ran

with it out of the bedroom toward the other side of the apartment.

6. Koury followed SIMMONS and ordered him to turn the SUBJECT COMPUTER over to Probation. After further discussion, SIMMONS handed the computer to Koury, who seized it and left the apartment. SIMMONS claimed that the computer belonged to his girlfriend, WINSOME WHITE. During an interview the next day, WHITE told Koury that the computer belonged to her and that SIMMONS had only used it once, to watch a movie.

7. Soon thereafter, Probation conducted a preliminary search of the computer to determine whether it contained evidence of conduct inconsistent with the terms of SIMMONS' supervised release. As a result of that search, Probation discovered evidence that the SUBJECT COMPUTER had been used to commit access-device fraud. In particular, Probation found that the computer contained evidence that the user of the computer had accessed an email account that reflected the purchase of goods from various merchants. Further investigation revealed that goods purchased using that same email account had been purchased using stolen credit card information.

8. On July 22, 2008, the Honorable Stephen C. Robinson, United States District Judge in the Southern District of New York, issued an order authorizing Probation to share

records relating to SIMMONS with any investigating agencies.

Accordingly, Probation provided the Secret Service and the United States Attorney's Office with a copy of a forensic report reflecting what Probation had found on the SUBJECT COMPUTER.

9. On May 29, 2009, SIMMONS, along with WINSOME WHITE, and others, was indicted by a grand jury sitting in this district for access-device fraud, in connection with a scheme to steal credit-card information and use that information to purchase airplane tickets and other goods. Many of those purchases were made online, using a computer. On July 13, 2009, SIMMONS pleaded guilty to one count of access-device fraud before the Honorable I. Leo Glasser. The trial of WINSOME WHITE is scheduled to begin on March 14, 2011.

10. Since Probation conducted its forensic review until February 24, 2011, the SUBJECT COMPUTER has remained in the possession of Probation, at which point it was delivered into the custody of the Secret Service and the U.S. Attorney's Office. It has not been tampered with, damaged or altered, and remains in the same condition as when seized on January 29, 2008.

11. Based upon the information set forth above, I believe that there is probable cause to believe that a search of the SUBJECT COMPUTER will contain evidence and instrumentalities of violations of Title 18, United States Code, Section 1029. By

this affidavit and application, I request that the Court issue a warrant allowing Secret Service agents to seize and search the SUBJECT COMPUTER.

III. Search Methodology to be Employed


12. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;

- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

WHEREFORE, I respectfully request that a search warrant issue, pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. §§ 2703(a), authorizing agents of the United States Secret Service and other law enforcement agents, to search the contents of the SUBJECT COMPUTER, and therein to seize the items described in Attachment A, all of

which constitute evidence, fruits, and instrumentalities of
violations of Title 18, United States Code, Section 1029.


MICHAEL ZAPPEL
Special Agent
United States Secret Service

Sworn to before me this
2nd day of March, 2011

-
e

Attachment A

List of Items to be Seized

All records and other stored information, in whatever form kept, constituting or showing evidence and instrumentalities of access-device fraud in violation of 18 U.S.C. § 1029(a), in the SUBJECT COMPUTER, including:

1. any and all stored e-mail, text messages, "chat," or instant messages, including any attachments to such e-mails or messages, sent by or received by the user(s) of the SUBJECT COMPUTER, whether saved or deleted, and whether contained directly in an e-mail, text message, chat, or instant message account or in a customized "folder";
2. any and all web-pages, internet browsing history, "cookies," and "bookmarks," including any associated links, that were created or maintained by the user(s) of the SUBJECT COMPUTER;
3. any and all spreadsheet, database, presentation, or word-processing files created or maintained by the user(s) of the SUBJECT COMPUTER, including but not limited to Excel, Access, PowerPoint, Publisher, Visio, Quicken, Word, Word Perfect, WordPad and Notepad files;
4. any and all video or sound files created or maintained by the user(s) of the SUBJECT COMPUTER;
5. any and all calendar, contact, or personal planner data or files, including but not limited to data contained in Outlook, Lotus Notes, or Eureka, created or maintained by the user(s) of the SUBJECT COMPUTER;
6. any and all contact information or call data relating to online voice or video communication services, including but not limited to Voice Over Internet Protocol (VOIP) communications on Skype or Vonage, created or maintained by the user(s) of the SUBJECT COMPUTER; and

7. any and all backup files for the items described²
above.